07-03-00

A

JC869 U.S. PTO 06/30/00

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000 OMB 0651-0032
Patent and Trademark Office: U S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	042390.P6758
First Inventor or Application Identifier	Paul C. Drews
Title	PROTECTED PLATFORM IDENTITY FOR DIGITAL SIGNING
Express Mail Label No.	EL466332145US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

JC542 U.S. PTO 09/608960 06/30/00

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [*Total Pages* 37]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 8]

4. Oath or Declaration [*Total Pages* 6]
a. ☒ Newly executed (original copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. ☐ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. ☐ Other: .....

**NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

16. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:

Prior application Information: *Examiner* _____ *Group/Art Unit:* _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* *or* ☒ *Correspondence address below*

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country	U.S.A.	*Telephone*	(714) 557-3800	*Fax*	(714) 557-3347

Name (Print/Type)	William W. Schaal, Reg. No. 39,018		
Signature		*Date*	06/30/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

BSTZ No. 042390.P6758
Express Mail No. EL466332145US

UNITED STATES PATENT APPLICATION

FOR

PROTECTED PLATFORM IDENTITY FOR DIGITAL SIGNING

Inventor:

PAUL C. DREWS

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Blvd., Suite 700
Los Angeles, California 90025
(714) 557-3800

BACKGROUND

1. FIELD

This invention relates to microprocessor. In particular, the invention relates to microprocessor cryptography.

2. GENERAL BACKGROUND

Advances in microprocessor and communication technologies have opened up many opportunities for applications that go beyond the traditional ways of doing business. Electronic commerce (E-commerce) and business-to-business (B2B) transactions are now becoming popular, reaching the global markets at a fast rate. Unfortunately, while modern microprocessor systems provide users convenient and efficient methods of doing business, communicating and transacting, they are also vulnerable to unscrupulous attacks. Examples of these attacks include virus, intrusion, security breach, and tampering. Computer security, therefore, is becoming more and more important to protect the integrity of the computer systems and increase the trust of users.

Threats caused by unscrupulous attacks may be in a number of forms such as passive wiretapping (eavesdropping), e.g., interception of messages, usually without detection, and active wiretapping (tampering), e.g., deliberate modification made to the message stream, which threatens authenticity. An invasive remote-launched attack by attackers may disrupt the normal operation

of a system connected to thousands or even millions of users. A virus program may corrupt code and/or data of a single-user platform.

Various efforts in the computer industry have been directed at improving security in computer processing environments. These efforts have been focused on various issues concerning data security including privacy, authentication, integrity, and non-repudiation, etc. Security solutions have been developed by various entities and companies in dealing with these basic security issues. In cases where software or other digital content is licensed to be used only on a specific system (e.g., platform) it is common to have the platform sign a unique message supplied by the content provider to "prove" that the platform identity matches the platform identity authorized to use the digital content. In cases where a platform originates a message or data it is common to have the platform sign the message or data to prove that the message or data originated from that platform.

The digital signature in these cases is produced using a private key. Ideally, the private key is kept secretly inside a platform (i.e., first platform) so that unauthorized users (e.g., intruders, attackers, forgers) cannot find out what it is. Unfortunately, signatures can be forged because if the authorized users can write code to use the private key, then the unauthorized users can also write code to read the private key and install it on another platform, allowing that other platform to impersonate the identity of the first platform.

Therefore, there is a need to have a technique to sign data with a high degree of resistance to attack that provides protection against a second

platform impersonating a first platform even if the attacker has access to the first platform.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1A is a diagram illustrating a block diagram of a protected authentication environment according to one embodiment of the invention

Figure 1B is a diagram illustrating a platform in which one embodiment of the invention can be practiced.

Figure 2 is a diagram illustrating a block diagram of the digital signature system shown in Figure 1A according to one embodiment of the invention.

Figure 3 is a diagram illustrating a block diagram of the protected authentication digital generator shown in Figure 2 according to one embodiment of the invention.

Figure 4 is a diagram illustrating a block diagram of the authentication identifier generator shown in Figure 1A according to one embodiment of the invention.

Figure 5 is a flowchart illustrating a process to generate a digital signature according to one embodiment of the invention.

Figure 6 is a flowchart illustrating the process shown in Block 540 of Figure 5 according to one embodiment of the invention.

Figure 7 is a flowchart illustrating a process to generate an authentication identifier according to one embodiment of the invention.

DETAILED DESCRIPTION

In the following description, for purposes of explanation, numerous details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that these specific details are not required in order to practice the present invention. In other instances, well-known electrical structures and circuits are shown in block diagram form in order not to obscure the present invention.

In the following description, terminology is used to discuss certain features of the present invention. For example, a "platform" includes hardware equipment and/or software that process information. Examples of a platform include, but are not limited or restricted to a computer (e.g., a desktop, a laptop, a hand-held, a server, a workstation, etc.), desktop office equipment (e.g., printer, scanner, a facsimile machine, etc.), a wireless telephone handset, a television set-top box, and the like. The term "information" is defined as one or more of data, address, and/or control.

With respect to cryptographic functionality, a key is information used by a cryptographic function to perform a particular operation such as encryption or

decryption. A "cryptographic function" is a software routine or a collective process for conducting cryptographic operations such as symmetric functions (e.g., Data Encryption Standard "DES"), asymmetric functions (e.g., Rivest, Shamir, and Adleman "RSA" based functions), or a function for digitally signing information (e.g., Digital Signature Algorithm "DSA" or a RSA-based signing functions). A "digital signature" is generally defined as data signal with a private key of the signatory. Normally, a digital signature is used to authenticate or verify data integrity in order to ensure that the data has not been illicitly modified after being digitally signed. The data may be provided in its entirety, or as a hash value produced by a hashing function. In addition, an "authentication vendor" is any person or entity in a position of trust to guarantee or sponsor certain information (e.g., a bank, government entity, trade association, original equipment manufacturer, etc.).

Figure 1A is a diagram illustrating an authentication system 100A according to one embodiment of the present invention. The authentication system 100A includes a first platform 100B, a second platform 100C, a digital signature system 120, an authentication identifier generator 130, and an authentication signature verifier 104.

The first platform 100B produces an authentication identifier 225 along with a corresponding public key 103. The public key 103 is a conventional asymmetric public key as is well known in the art. The authentication identifier 225 is similar to a corresponding private key, except that it has been altered so that it can only be used on the specific second platform 100C for generating a digital signature 105.

The second platform 100C is a platform on which the digital signature 105 and data 102 are generated. The second platform 100C is typically used or accessed by a user who desires to generate the digital signature 105 to prove the origin and integrity of data 102. The data 102 may be numbers, a text file, a program, a picture file, an audio file, a media file, an electronic mail (e-mail), a hyper-text markup language (HTML) page, document, etc.

In one common usage, the data 102 is a unique message supplied by a provider of digital content or software licensed only for use on the specific second platform 100C. The second platform 100C generates the digital signature 105 of the supplied data to prove the identity of the platform to a digital content or software provider.

The digital signature 105 can be verified using the authentication signature verifier 104. Verification is performed using the public key 103 according to public-key based digital signature verification techniques that are well known in the art. The verification of the digital signature 105 may be performed inside or outside the second platform 100C.

The authentication identifier generator 130 generates both (i) the authentication identifier 225 to be used by the protected authentication signature generator 230 and (ii) a corresponding public key 103 to be used by the authentication signature verifier 104. The authentication identifier generator 130 is external to the second platform 100C and is provided by an authentication vendor. The generation of the authentication identifier 225 is shown in Figure 4. The second platform 100C receives the authentication identifier 225 and uses the digital signature system 120 to generate the digital

signature 105. The digital signature system 120 may be implemented inside or outside of the second platform 100C.

The authentication identifier generator 130 and the protected authentication signature generator 230 may be implemented by hardware, software, or any combination thereof.

Figure 1B is a diagram illustrating a platform in which one embodiment of the present invention can be practiced. The first platform 100B or the second platform 100C includes a processor 101, a host bus 111, a host bridge chipset 121, a system memory 132, a primary peripheral component interconnect (PCI) bus 151, PCI slots 161_1 to 161_K ("K" $\geq$ 2), a PCI-to-industry standard architecture (ISA) bridge 172, mass storage device 173, Input/Output (I/O) ports 171, an ISA bus 182, and ISA slots 181_1 to 181_M ("M" $\geq$ 2).

The processor 101 represents a processing unit of any type of architecture. For example, the processor 101 may be implemented as a microcontroller, a digital signal processor, a state machine, or a central processing unit (CPU). The CPU may be implemented with a variety of architecture types such as complex instruction set computers (CISC), reduced instruction set computers (RISC), very long instruction word (VLIW), or hybrid architecture.

The host bridge chipset 121 includes a number of interface circuits to allow the processor 101 access to the system memory 132 and the primary PCI bus 151. The system memory 132 represents one or more mechanisms for storing information. For example, the system memory 132 may include non-volatile or volatile memories. Examples of these memories include flash

memory, read only memory (ROM), or random access memory (RAM). In the platform 100B, the system memory 132 may contain a program that can implement the authentication identifier generator 130 and other programs or data. In the platform 100C, the system memory may contain a program that can implement a protected authentication signature generator program 230 and other programs and data. The program in the platform may be software program or firmware program. Of course, the system memory 132 preferably contains additional software (not shown), which is not necessary to understanding the invention.

The PCI slots 161_1 to 161_K provide interfaces to PCI devices. Examples of PCI devices include the network interface and the media interface. The network interface connects to communication channel such as the Internet. The Internet provides access to on-line service providers, Web browsers, and other network channels. The media interface provides access to audio and video devices.

The PCI-to-ISA bridge 172 provides access to the ISA bus 182, mass storage devices 173, and input/output (I/O) ports 171. The I/O ports 171 provides interface to I/O devices (not shown). The I/O devices may include any I/O devices to perform I/O functions such as a media card (e.g., audio, video, graphics), a network card and the like. The mass storage device 173 includes a machine readable media such as a compact disk (CD) ROM, a digital video disk (DVD), ZIP™ disk, floppy diskette, hard drive, and the like. The mass storage device 173 stores archive information such as code, programs, files,

and operating systems. The mass storage device 173 provides a mechanism to read the machine-readable media.

When implemented in software, the elements of the present invention are the code segments to perform the necessary tasks. The program or code segments can be stored in a processor readable medium or transmitted by a computer data signal embodied in a carrier wave, or a signal modulated by a carrier, over a transmission medium. The "processor readable medium" may include any medium that can store or transfer information. Examples of the processor readable medium include an electronic circuit, a semiconductor memory device, a ROM, a flash memory, an erasable programmable ROM (EPROM), a floppy diskette, a CD-ROM, an optical disk, a hard disk, a fiber optical medium, a radio frequency (RF) link, etc. The computer data signal may include any signal that can propagate over a transmission medium such as electronic network channels, optical fibers, air, electromagnetic, RF links, etc. The code segments may be downloaded via computer networks such as the Internet, an Intranet, etc. The ISA bus 182 has a number of ISA slots 181_1 to 181_M to interface to ISA devices. Examples of ISA devices include data entry devices (e.g., keyboard, mouse, trackball, pointing device), printers, etc.

The protected authentication signature generator 230 may be stored in ROM to guard against attacks that forge a digital signature of a different platform. The protected authentication signature generator 230 may be retrieved from a processor readable medium or transmission medium. In this case, it is common to use a digital signature of the program or code segments to guard against alteration attacks. Such digital signature techniques are well known in the art.

Figure 2 is a diagram illustrating a block diagram of the digital signature system 120 according to one embodiment of the invention. The digital signature system 120 includes a first storage 210, a second storage 220, and a protected authentication signature generator 230. The protected authentication signature generator 230 signs the data 102 to generate digital signature 105 using the unique platform identifier 215 and the authentication identifier 225.

The first storage 210 guards against the unique platform identifier 215 being easily altered. In one embodiment, the unique platform identifier 215 is a platform identifier (ID) "Universal Unique Identifier" (UUID) or "Globally Unique Identifier" (GUID) retrieved from a System Management Basic Input/Output System (SMBIOS) table. Techniques for generating such unique identifiers, storing them in an SMBIOS table, and guarding them against alteration are well known in the industry.

In another embodiment, the unique platform identifier 215 is a unique processor serial number retrieved using a special processor instruction. The processor guards against its internal serial number being altered. Any digital platform identifier can be used as long as it is unique and guarded against alteration.

The second storage 220 stores the authentication identifier 225. Unique to the second platform 100C, the authentication identifier 225 is provided by the authentication vendor and is installed to the platform 100C (shown in Figure 4). Since the authentication identifier 225 may be dynamically installed in the platform 100C after the platform is manufactured, it is likely that the second storage 220 is not guarded or cannot be guarded against being altered.

However, the present invention protects against the authentication identifier 225 being used to generate any valid digital signatures if it has been altered.

The protected authentication signature generator 230 is used to prove the originator (e.g., platform) and integrity of a message. The protected authentication signature generator 230 represents a black box or a function that is transparent to the users. The origination and integrity proof is created when a user from the platform 100C performs the signing function via the protected authentication signature generator 230 that is unique to the platform 100C. This signing function produces the digital signature 105.

Referring back to Figure 1A, the authentication signature verifier 104 completes the authentication cycle by verifying that data is unaltered compared to the data from which the digital signature is computed and that the digital signature 105 is generated by the correct platform 100C. The authentication signature verifier 104 takes as input the data 102, the digital signature 105, and the public key 103. The authentication signature verifier 104 generates as output an information bit signifying whether or not the data matches the original data and the digital signature is generated using the corresponding private key.

In one embodiment, the digital signature 105 and the data 102 are collected into a single "signed data" message. The data 102 and the digital signature 105 may have any type of format and may or may not be collected into a single message.

Figure 3 is a diagram illustrating the protected authentication signature generator 230 shown in Figure 2 according to one embodiment of the invention. The protected authentication signature generator 230 includes a platform-specific transformer 310, a decryptor 320, and a signer 330.

The platform-specific transformer 310 performs a platform-specific transformation of the authentication identifier 225 to output an encrypted platform private key 315. The transformation uses the unique platform identifier 215 to make the transformation unique to the platform. The platform-specific transformation is reversible in the sense that the opposite transformation from the encrypted platform private key 315 to the authentication identifier 225 can be readily done given the same unique platform identifier 215. Any of a variety of different embodiments of the platform-specific transformer 310 can be used as long as they have the required properties of being reversible and being specific to the unique platform identifier 215.

For example, the platform-specific transformer 310 may be an Exclusive OR (XOR) device that performs a bit-wise XOR of two input streams of bits to produce an output stream of bits. One of the input bit streams is the authentication identifier 225. The other input bit stream is a unique, serially uncorrelated bit stream generated in a reproducible way from the unique platform identifier 215. In one embodiment of the serially uncorrelated bit stream, a cryptographic hash of the unique platform identifier 215 is computed to generate the first run of bits. As long as more bits are needed, the previous run of bits is hashed to produce the next run of bits.

In another embodiment of the platform-specific transformer 310, the unique platform identifier 215 is used as a seed to generate a symmetric encryption/decryption key, and the transformation is a decryption using this symmetric key. Techniques for generation of symmetric keys and symmetric key decryption from the unique platform identifier 215 are well known in the art.

The platform-specific transformer 310 further includes a reporting device 340 to report the unique platform identifier 215 that is used in the transformation. The reporting device 340 generates an additional output from the protected authentication signature generator 230. The additional output is referred to as the "tracked platform identifier" 216, which may be simply a copy of the unique platform identifier 215. For example, this may be used to detect attacks based on forging or altering the platform's unique platform identifier 215. If the same tracked platform identifier 216 is detected from several different platforms, a forgery may be detected.

The decryptor 320 decrypts the encrypted platform private key 315 to generate a "clear" copy of the platform private key 335. The decryption is an asymmetric decryption performed using an authentication identifier generator's public key 325 embedded in the protected authentication signature generator 230. The authentication identifier generator's pubic key 325 is provided to the platform 100C by the vendor of the authentication identifier 225 (e.g., authentication vendor). The authentication identifier generator's public key 325 is a "public" key of the asymmetric encryption public/private key pair used by the authentication vendor.

The inclusion of the decryptor 320 in the protected authentication signature generator 230 provides protection against attacks based on reverse-engineering the protected authentication signature generator 230. Without the decryptor 320, a skilled attacker could use the reverse of the transformation by the platform-specific transformer 310 transformation to compute and then install the authentication identifier 225 that would be suitably transformed into a desired platform private key 335. With the decryptor 320 present, the attacker

would have to break the encryption algorithm or the private key corresponding to the authentication identifier generator's public key 325. Since the security of an algorithm rests in the key, it is important that the authentication identifier generator's public key 325 and its corresponding private key be generated using a strong cryptographic process.

The protected authentication signature generator 230 may be exposed to reverse-engineering. In this case, security of the invention depends on how resistant the protected authentication signature generator 230 and the unique platform identifier 215 are to duplication and modification. In other cases, the protected authentication signature generator 230 is protected against reverse-engineering. In these cases the authentication identifier generator's public key 325 and the platform private key 335 are secret. This provides protection against an attacker being able to build an alternate device or software module that can produce equivalent signatures.

The signer 330 generates a digital signature 105 of the data 102 using the platform private key 335. The platform private key 335 is the "private" member of an asymmetric public/private key pair to be used for generation and verification of digital signatures using any of a variety of algorithms. Example algorithms include ElGama, Schnorr and Digital Signature Algorithms schemes just to name a few. However, it is not required that these keys also be usable for bulk data encryption and decryption.

The unique platform identifier 215 is a permanent identifier, and may be generated and stored at the time of manufacturing or the initial system boot of the platform 100C. For example, the unique platform identifier 215 may be programmed into fuses of a system ROM. The authentication identifier 225 is

provided by the authentication vendor and may be stored at the time of manufacturing or an initial first system boot. However, the present invention allows the authentication identifier 225 to be stored later in the lifetime of the system, and possibly altered if desired. In general, this means that the authentication identifier 225 will be stored in a place where someone could read it and copy it to another platform. However, the copied authentication identifier 225 will not be usable on another platform other than the platform 100C. The platform-specific transformer 310 on the another platform transforms the copied authentication identifier 225 to a different encrypted platform private key 315, the decryptor 320 decrypts it to an invalid platform private key 335, and the signer 330 will either generate an incorrect digital signature 105 or refuse to perform the operation at all depending on its design.

Figure 4 is a diagram illustrating the authentication identifier generator 130 shown in Figure 1A according to one embodiment of the invention. The authentication identifier generator 130 includes an encryptor 410 and a platform-specific reverse transformer 420.

The platform private key 335 and the corresponding platform public key 103 may be generated by the user (e.g., purchaser) and the platform private key 335 is then supplied to the authentication vendor. The platform private key 335 and the corresponding platform public key 103 may also be generated by the authentication vendor and the platform public key 103 is then supplied to the user.

The encryptor 410 encrypts the platform private key 335 to generate an encrypted platform private key 315 using an authentication identifier generator's private key 415 owned by the authentication vendor. The encryptor 410

performs the reverse of the decryption performed by the decryptor 320 shown in Figure 3. When the protected authentication signature generator is exposed to reverse-engineering, the encryptor 410 and decryptor 320 use asymmetrical encryption and decryption. Symmetrical encryption and decryption may be used if there is no risk that either the encryptor 410 or decryptor 320 may be reverse-engineered.

The platform-specific reverse transformer 420 transforms the encrypted private key 315 to generate the authentication identifier 225. The platform-specific reverse transformer 420 uses the unique platform identifier 215 to make its transformation platform-specific. The platform-specific reverse transformer 420 performs the exact reverse of the transformation performed by the platform-specific transformer 310 shown in Figure 3.

Any of a variety of embodiments of the platform-specific reverse transformer 420 can be used as long as the embodiment used is the reverse of the platform-specific transformer 310. If the XOR embodiment of the platform-specific transformer 310 is used, the identical algorithm can be used for the platform-specific reverse transformer 420. The platform-specific transformer 310 that uses symmetric-key decryption may need to use an encryption variation of the algorithm for the platform-specific reverse transformer 420.

Figure 5 is the flowchart illustrating a process 500 to generate a signed data according to one embodiment of the invention.

Upon START, the process 500 retrieves the unique platform identifier from the first storage (Block 510). Then the process 500 retrieves the authentication identifier from the second storage (Block 520). Next, the process 500 receives data that needs to be signed by the platform (Block 530).

The process 500 generates a digital signature using the unique platform identifier and the authentication identifier (Block 540). The signed data is a digital code that is the output result of the process 500. Then the process 500 is terminated.

Figure 6 is a flowchart illustrating the process generating the digital signature of process 500 according to one embodiment of the invention.

Upon START, the process 540 transforms the authentication identifier and the platform identifier to generate an encrypted platform private key (Block 610). The transformation is a reversible transformation that uses the unique platform identifier to make the transformation platform-specific. Next, the process 540 decrypts the encrypted platform private key using the using an authentication identifier generator's public key, producing a platform private key (Block 620). Then, the process 540 generates a digital signature for the data using the platform private key (Block 630) according to digital signature generation algorithms. Then the process 540 is terminated.

Figure 7 is a flowchart illustrating a process 700 to generate an authentication identifier according to one embodiment of the invention.

Upon START, the process 700 obtains a platform private key (Block 710). Then, the process 700 obtains an authentication identifier generator's private key (Block 720). Next, the process 700 encrypts the platform private to generate an encrypted platform private key using the authentication identifier generator's private key (Block 730). The process 700 obtains a unique platform identifier from the platform (Block 740). Then the process 700 transforms the encrypted platform private key to generate an authentication identifier (Block 750). The transformation is made platform-specific by the use of the unique

platform identifier, and is the reverse of the transformation of Block 610. Then the process 700 is terminated.

While this invention has been described with reference to illustrative embodiment, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. An apparatus comprising:

a first storage to store a platform identifier unique to a platform;

a second storage to store an authentication identifier, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

a signature generator to generate a digital signature for data using the platform identifier and the authentication identifier.

2. The apparatus of claim 1 wherein the signature generator comprises:

a platform-specific transformer to transform the authentication identifier using the platform identifier to output an encrypted platform private key; and

a decryptor coupled to the platform-specific transformer to decrypt the encrypted platform private key to generate the platform private key using an authentication public key, the authentication public key being provided by the authentication vendor.

3. The apparatus of claim 2 wherein the signature generator further comprises:

a signer coupled to the decryptor to sign the data using the platform private key, the platform private key being transparent to the platform.

4. The apparatus of claim 2 wherein the platform-specific transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the platform identifier and the authentication identifier.

5. The apparatus of claim 2 wherein the platform-specific transformer comprises:

a decryptor to decrypt the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

6. The apparatus of claim 2 wherein the authentication identifier is generated by a platform-specific reverse transformer which transforms the encrypted platform private key using the platform identifier, the encrypted platform private key being encrypted from the platform private key using the authentication private key.

7. The apparatus of claim 6 wherein the platform-specific reverse transformer comprises an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key using the platform identifier.

8. The apparatus of claim 4 wherein the platform identifier is a unique, serially uncorrelated bit stream.

9. The apparatus of claim 6 wherein the platform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated from the platform identifier.

10. The apparatus of claim 1 wherein the platform identifier is installed in the first storage in a protected environment.

11. The apparatus of claim 10 wherein the protected environment is a system management basic input/output system table.

12. The apparatus of claim 4 wherein the platform-specific transformer further comprises:

a reporting device to report the platform identifier to generate a tracked platform identifier.

13. The apparatus of claim 1 wherein the platform identifier is a processor serial number retrieved from a processor.

14. An apparatus comprising:

an encryptor to encrypt a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and

a platform-specific reverse transformer to transform the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform, the authentication identifier being provided to the platform to generate a digital signature.

15. The apparatus of claim 14 wherein the platform-specific reverse transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

16. The apparatus of claim 15 wherein the platform identifier is a unique, serially uncorrelated bit stream.

17. The apparatus of claim 14 wherein the platform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

18. A method comprising:

storing a platform identifier unique to a platform and an authentication identifier in first and second storages, respectively, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

generating a digital signature for data using the platform identifier and the authentication identifier.

19. The method of claim 18 wherein generating digital signature comprises:

transforming the authentication identifier using the platform identifier to output an encrypted platform private key; and

decrypting the encrypted platform private key to generate the platform private key using an authentication public key provided by the authentication vendor.

20. The method of claim 19 wherein generating the digital signature further comprises:

signing the data using the platform private key, the platform private key being transparent to the platform.

21. The method of claim 19 wherein transforming the authentication identifier comprises:

performing an Exclusive OR (XOR) function on the platform identifier and the authentication identifier.

22. The method of claim 19 wherein transforming the authentication identifier comprises:

decrypting the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

23. The method of claim 19 wherein the authentication identifier is generated by transforming the encrypted private key using the platform identifier, the encrypted private key being encrypted from the platform private key using an authentication private key.

24. The method of claim 23 wherein transforming the encrypted private key using the platform identifier comprises performing an XOR function on the encrypted platform private key and the platform identifier.

25. The method of claim 21 wherein the platform identifier is a unique, serially uncorrelated bit stream.

26. The method of claim 23 wherein transforming the encrypted private key comprises encrypting the encrypted private key using a symmetric encryption/decryption key generated from the platform identifier.

27. The method of claim 18 wherein storing the platform identifier comprises installing the platform identifier in a protected environment.

28. The method of claim 27 wherein the protected environment is a system management basic input/output system table.

29. The method of claim 21 wherein transforming the authentication identifier further comprises:

reporting the platform identifier to report a tracked platform identifier.

30. The method of claim 18 wherein the platform identifier is a processor serial number retrieved from a processor.

31. A method comprising:

encrypting a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and

transforming the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform.

32. The method claim 31 wherein transforming the encrypted platform private key comprises:

performing an Exclusive OR (XOR) function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

33. The method of claim 32 wherein the platform identifier is a unique, serially uncorrelated bit stream.

34. The method of claim 31 wherein transforming the encrypted platform private key comprises encrypting the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

35. A computer program product comprising:

a machine readable medium having computer program code therein, the computer program product comprising:

computer readable program code for storing a platform identifier unique to a platform and an authentication identifier in first and second storages, respectively, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

computer readable program code for generating a digital signature for data using the platform identifier and the authentication identifier.

36. The computer program product of claim 35 wherein the computer readable program code for generating digital signature comprises:

computer readable program code for transforming the authentication identifier using the platform identifier to output an encrypted platform private key; and

computer readable program code for decrypting the encrypted platform private key to generate the platform private key using an authentication public key provided by the authentication vendor.

37. The computer program product of claim 36 wherein the computer readable program code for generating the digital signature further comprises:

computer readable program code for signing the data using the platform private key, the platform private key being transparent to the platform.

38. The computer program product of claim 36 wherein a computer readable program code for transforming the authentication identifier comprises:

computer readable program code for performing an Exclusive OR (XOR) function on the platform identifier and the authentication identifier.

39. The computer program product of claim 36 wherein a computer readable program code for transforming the authentication identifier comprises:

computer readable program code for decrypting the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

40. The computer program product of claim 36 wherein the authentication identifier is generated by a computer readable program code for transforming the encrypted private key using the platform identifier, the encrypted private key being encrypted from the platform private key using an authentication private key.

41. The computer program product of claim 40 wherein a computer readable program code for transforming the encrypted private key and the platform identifier comprises performing an XOR function on the encrypted platform private key and the platform identifier.

42. The computer program product of claim 38 wherein the platform identifier is a unique, serially uncorrelated bit stream.

43. The computer program product of claim 40 wherein a computer readable program code for transforming the encrypted private key comprises a computer readable program code for encrypting the encrypted private key using a symmetric encryption/decryption key generated from the platform identifier.

44. The computer program product of claim 35 wherein the computer readable program code for storing the platform identifier comprises computer readable program code for installing the platform identifier in a protected environment.

45. The computer program product of claim 44 wherein the protected environment is a system management basic input/output system table.

46. The computer program product of claim 38 wherein a computer readable program code for transforming the authentication identifier further comprises:

computer readable program code for reporting the platform identifier to generate a tracked platform identifier.

47. The computer program product of claim 35 wherein the platform identifier is a processor serial number retrieved from a processor.

48. A computer program product comprising:

a machine readable medium having computer program code therein, the computer program product comprising:

computer readable program code for encrypting a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and

computer readable program code for transforming the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform.

49. The computer program product claim of 48 wherein a computer readable program code for transforming the encrypted platform private key comprises:

computer readable program code for performing an Exclusive OR (XOR) function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

50. The computer program product of claim 49 wherein the platform identifier is a unique, serially uncorrelated bit stream.

51. The computer program product of claim 48 wherein the computer readable program code for transforming the encrypted platform private key comprises computer readable program code for encrypting the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

52. A system comprising:

a platform having a unique platform identifier (ID); and

a digital signature system coupled to the platform to authenticate data, the digital signature system comprising:

a first storage to store the platform identifier;

a second storage to store an authentication identifier, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

a signature generator to generate a digital signature for data using the platform identifier and the authentication identifier.

53. The system of claim 52 wherein the signature generator comprises:

a platform-specific transformer to transform the authentication identifier using the platform identifier to output an encrypted platform private key; and

a decryptor coupled to the platform-specific transformer to decrypt the encrypted platform private key to generate the platform private key using an authentication public key, the authentication public key being provided by the authentication vendor.

54. The system of claim 53 wherein the signature generator further comprises:

a signer coupled to the decryptor to sign the data using the platform private key, the platform private key being transparent to the platform.

55. The system of claim 53 wherein the platform-specific transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the platform identifier and the authentication identifier.

56. The system of claim 53 wherein the platform-specific transformer comprises:

a decryptor to decrypt the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

57. The system of claim 53 wherein the authentication identifier is generated by a platform-specific reverse transformer which transforms the encrypted platform private key and the platform identifier, the encrypted platform private key being encrypted from the platform private key using the authentication private key.

58. The system of claim 57 wherein the platform-specific reverse transformer comprises an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key and the platform identifier.

59. The system of claim 55 wherein the platform identifier is a unique, serially uncorrelated bit stream.

60. The system of claim 57 wherein the platform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated from the platform identifier.

61. The system of claim 52 wherein the platform identifier is installed in the first storage in a protected environment.

62. The system of claim 61 wherein the protected environment is a system management basic input/output system table.

63. The system of claim 55 wherein the platform-specific transformer further comprises:

a reporting device to report the platform identifier to generate a tracked platform identifier.

64. The system of claim 52 wherein the platform identifier is a processor serial number retrieved from a processor.

65. A system comprising:

a digital signature system;

an authentication identifier generator coupled to the digital signature system, the authentication identifier generator comprising:

an encryptor to encrypt a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and

a platform-specific reverse transformer to transform the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform, the authentication identifier being provided to the platform to generate a digital signature.

66. The system of claim 65 wherein the platform-specific reverse transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

67. The system of claim 66 wherein the platform identifier is a unique, serially uncorrelated bit stream.

68. The of system claim 65 wherein the transform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

a first storage to store a platform identifier unique to a platform;

a second storage to store an authentication identifier, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

a signature generator to generate a digital signature for data using the platform identifier and the authentication identifier.

ABSTRACT

A first storage to store a platform identifier (ID). The platform ID is unique to a platform. A second storage to store an authentication identifier. The authentication identifier is provided by an authentication vendor. The authentication vendor uses the platform ID, a platform private key, and an authentication private key. A signature generator uses the platform ID and the authentication identifier to generate a digital signature.

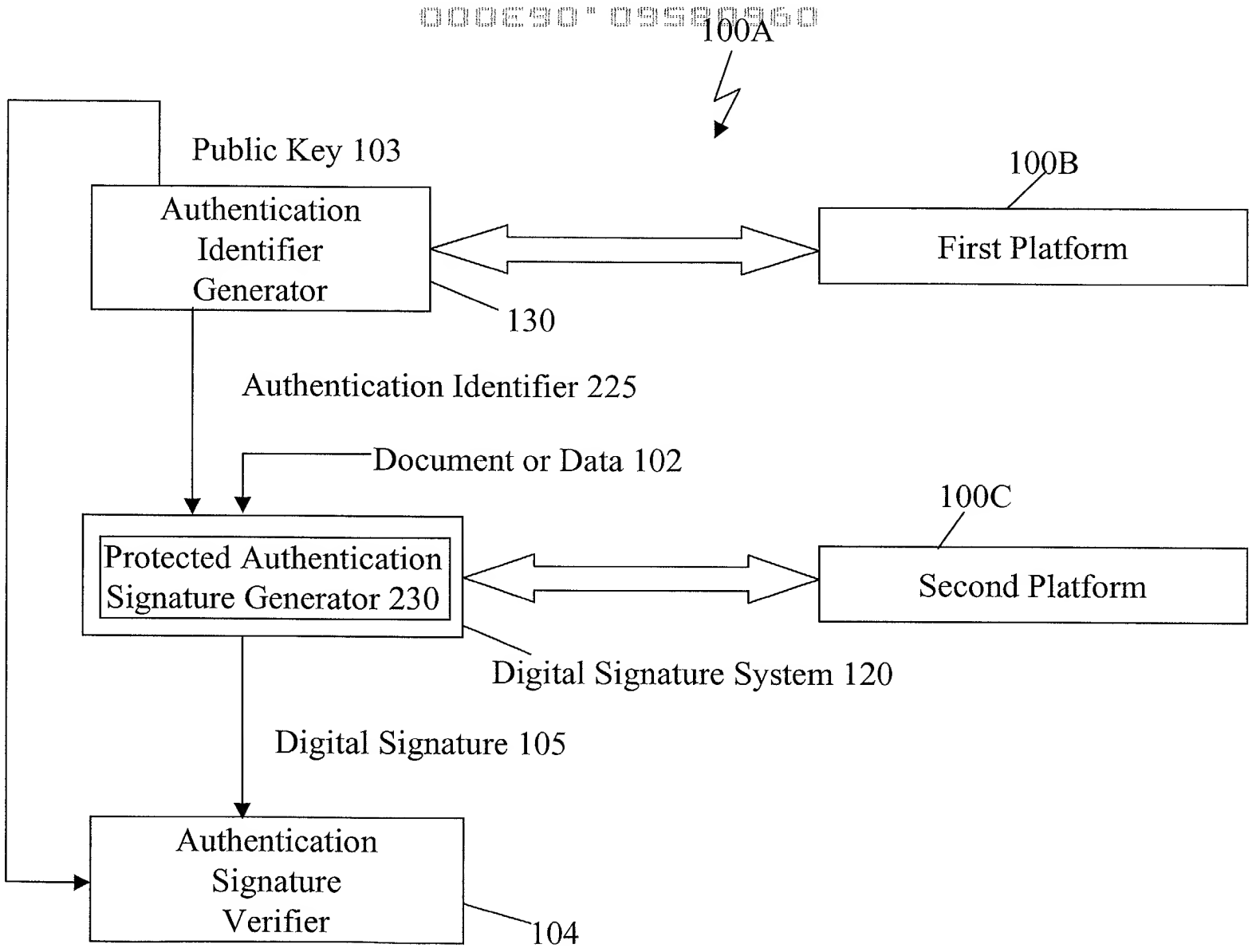
100A
Public Key 103
Authentication Identifier Generator
130
100B
First Platform
Authentication Identifier 225
Document or Data 102
Protected Authentication Signature Generator 230
100C
Second Platform
Digital Signature System 120
Digital Signature 105
Authentication Signature Verifier
104

Fig. 1A

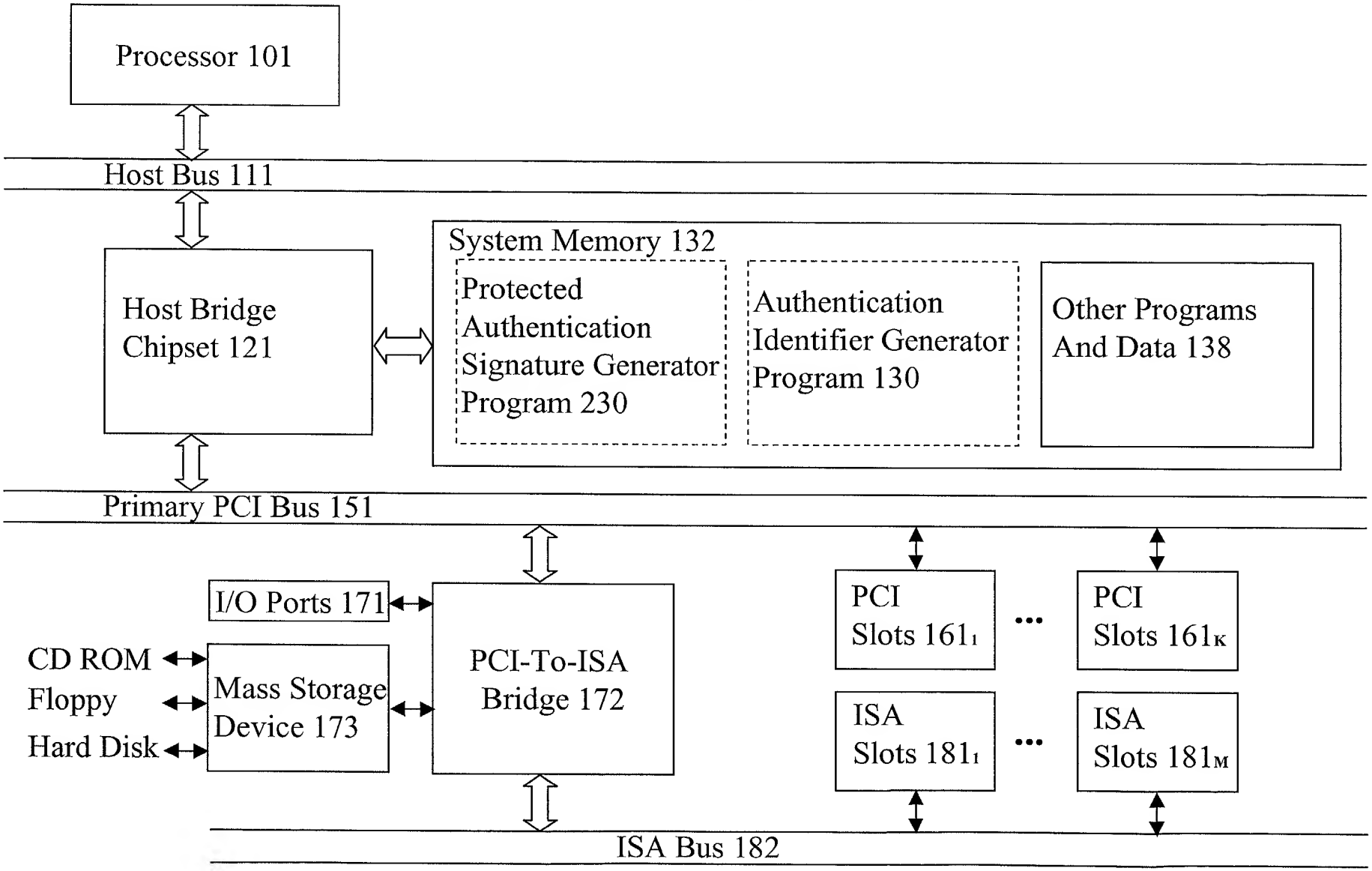

Fig. 1B

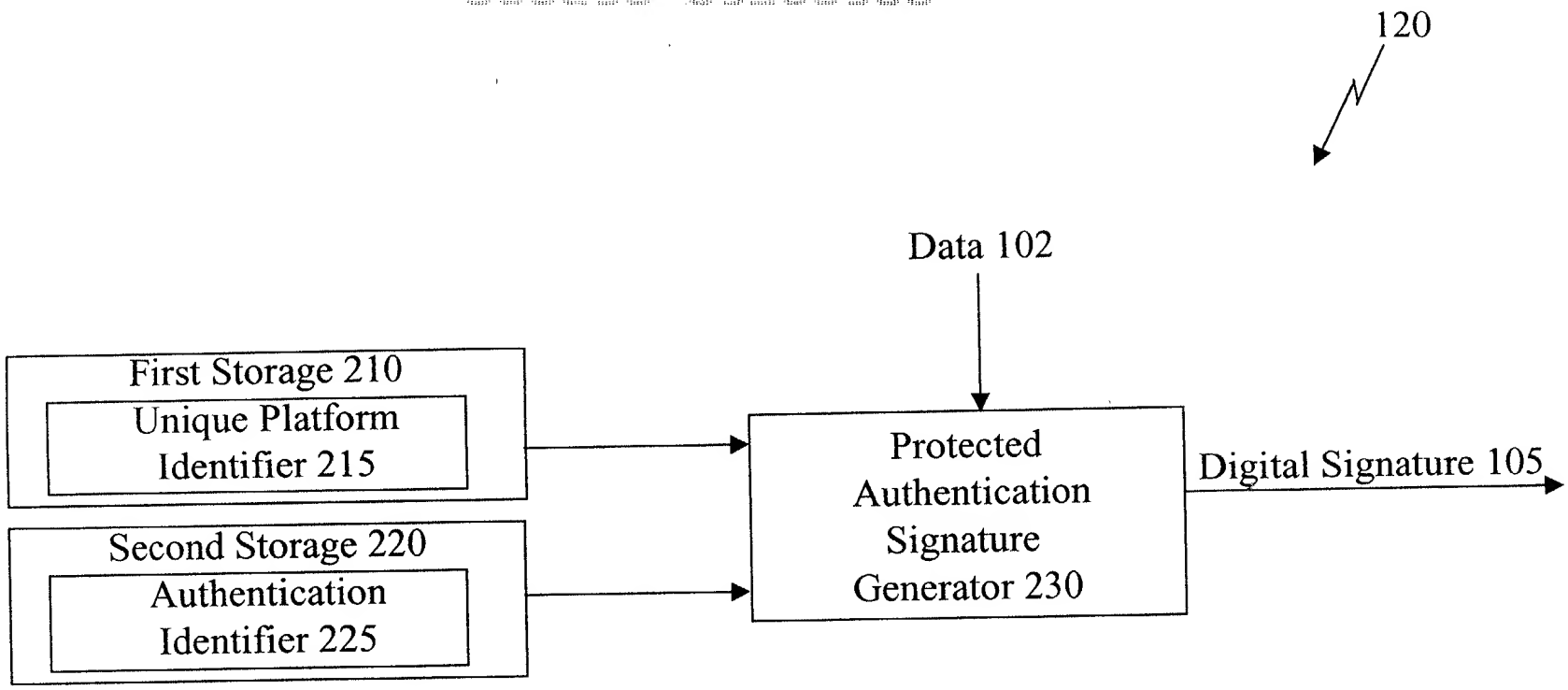
120
Data 102
First Storage 210
Unique Platform Identifier 215
Second Storage 220
Authentication Identifier 225
Protected Authentication Signature Generator 230
Digital Signature 105

Fig. 2

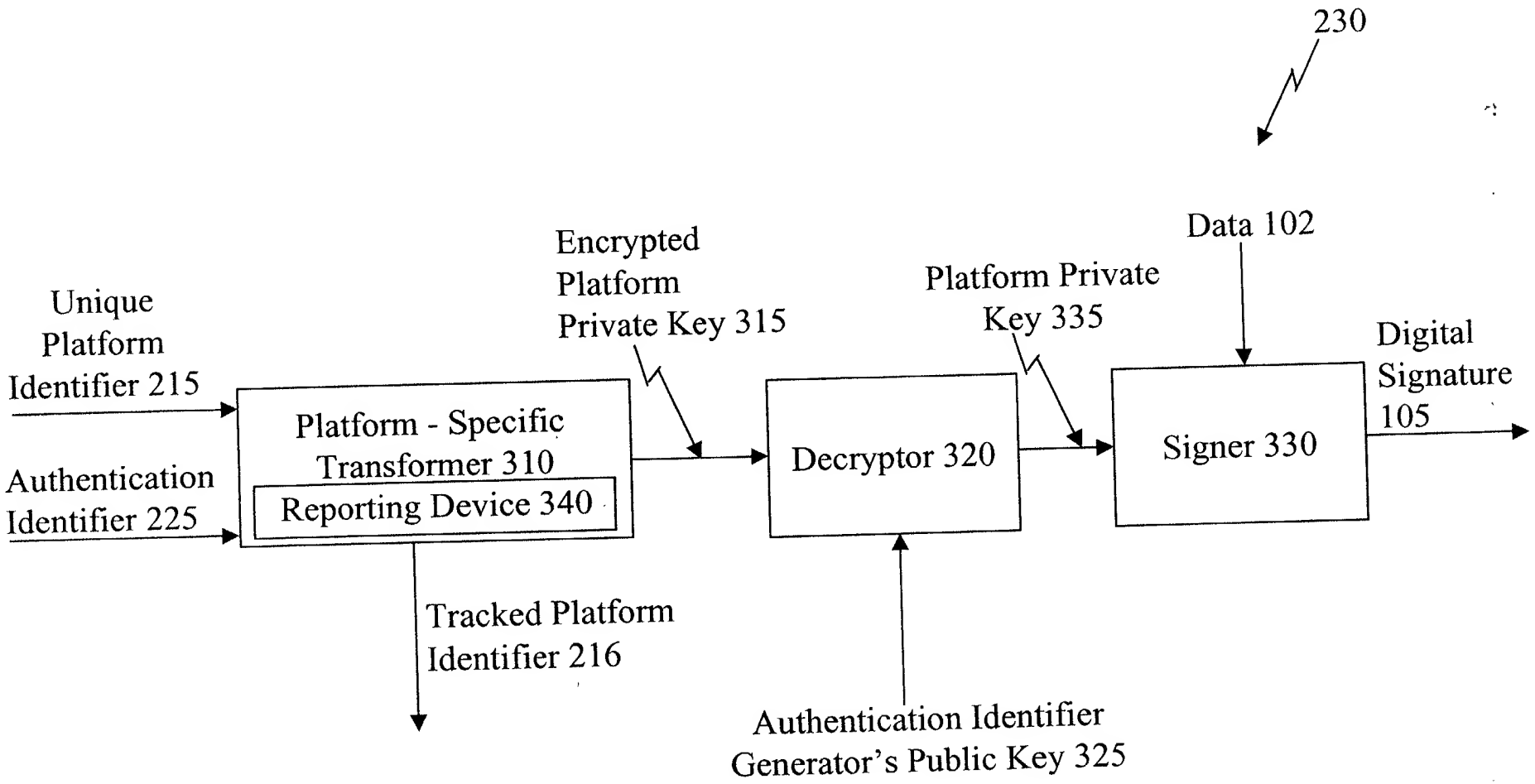
230
Unique Platform Identifier 215
Authentication Identifier 225
Platform - Specific Transformer 310
Reporting Device 340
Encrypted Platform Private Key 315
Decryptor 320
Platform Private Key 335
Data 102
Signer 330
Digital Signature 105
Tracked Platform Identifier 216
Authentication Identifier Generator's Public Key 325

Fig. 3

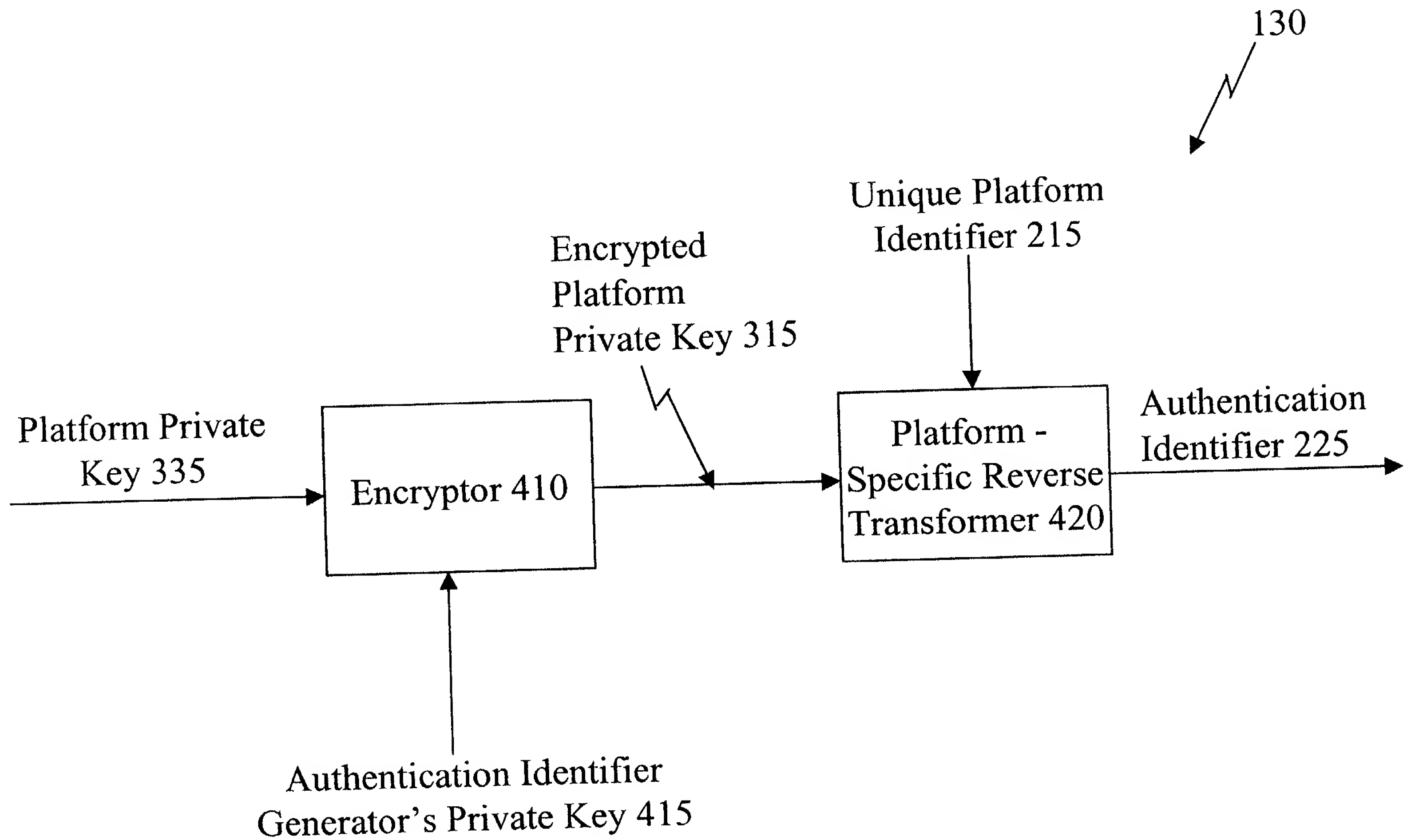

Fig. 4

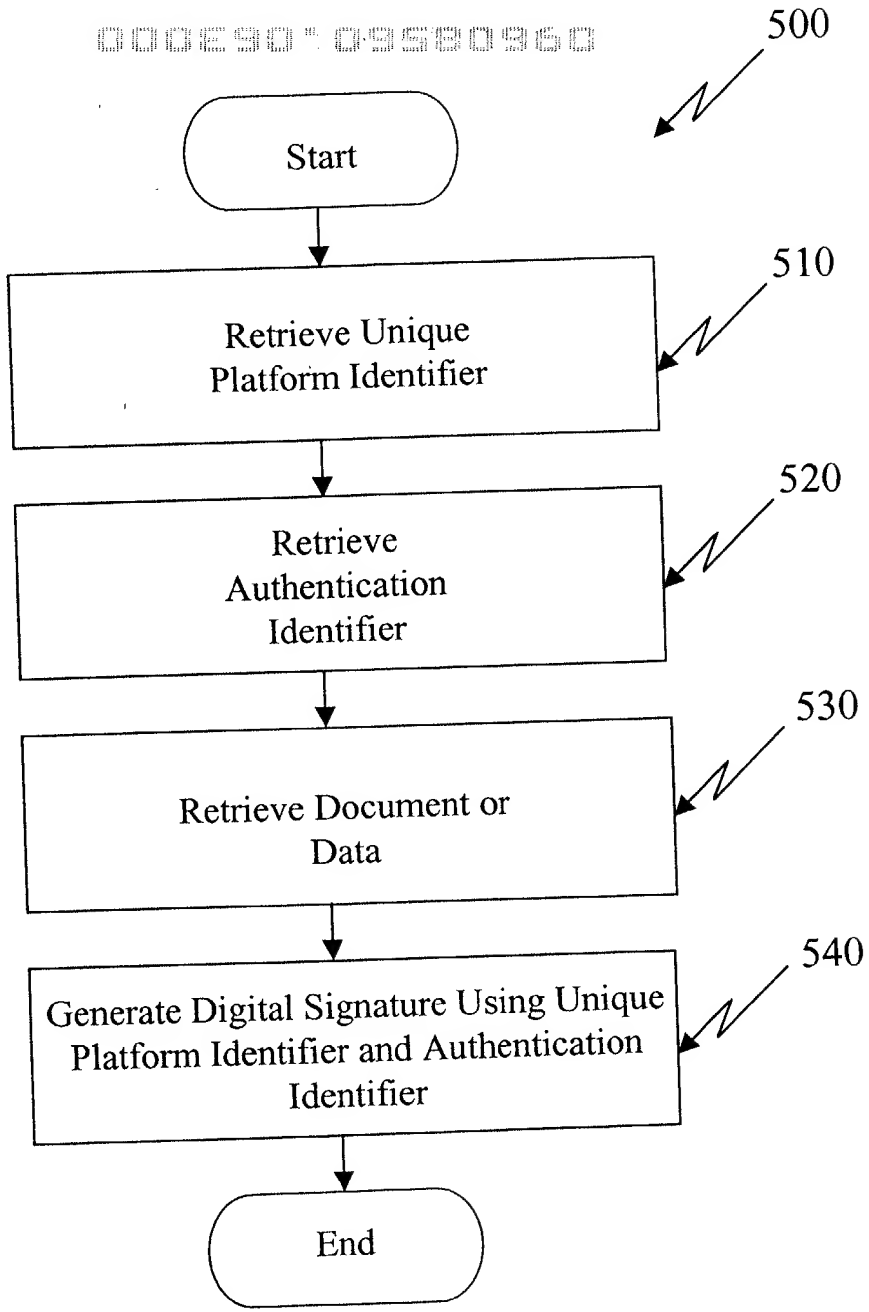
500
Start
510
Retrieve Unique Platform Identifier
520
Retrieve Authentication Identifier
530
Retrieve Document or Data
540
Generate Digital Signature Using Unique Platform Identifier and Authentication Identifier
End

Fig. 5

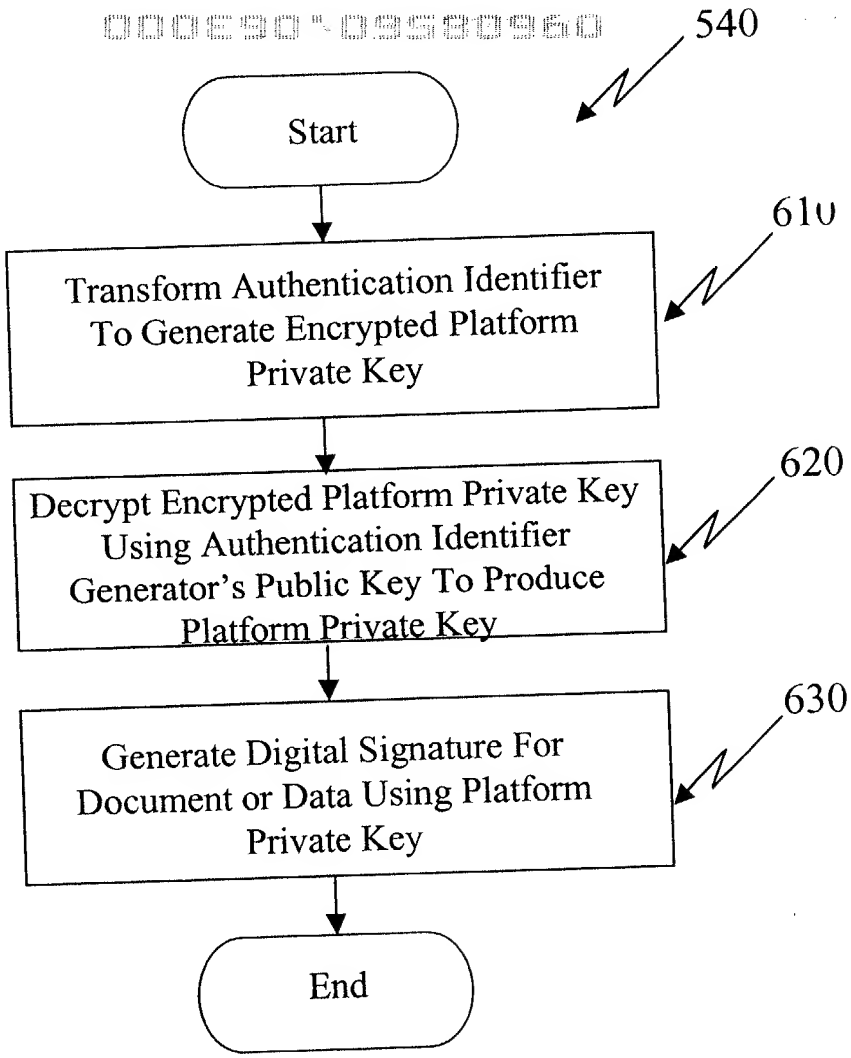
540
Start
610
Transform Authentication Identifier To Generate Encrypted Platform Private Key
620
Decrypt Encrypted Platform Private Key Using Authentication Identifier Generator's Public Key To Produce Platform Private Key
630
Generate Digital Signature For Document or Data Using Platform Private Key
End

Fig. 6

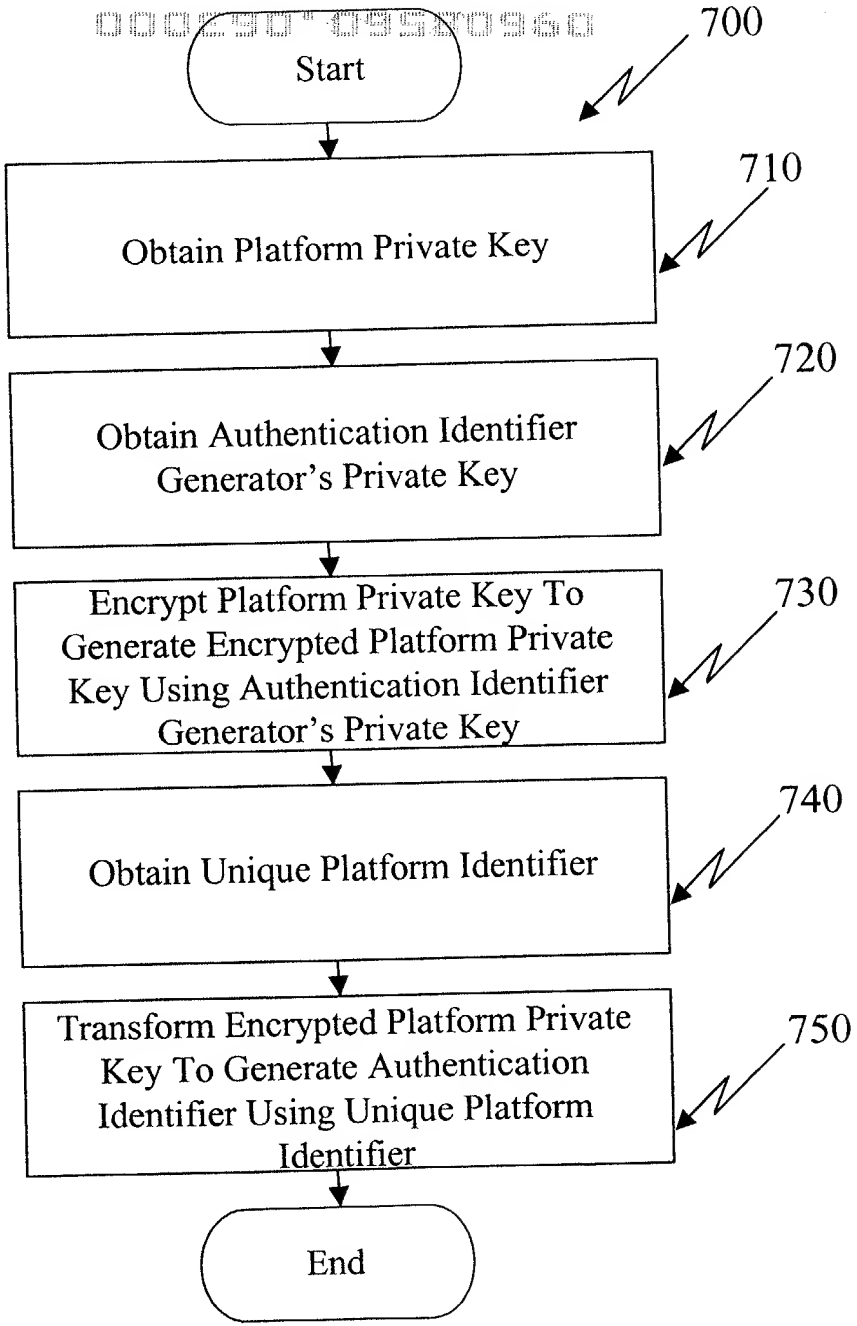
700
Start
710
Obtain Platform Private Key
720
Obtain Authentication Identifier Generator's Private Key
730
Encrypt Platform Private Key To Generate Encrypted Platform Private Key Using Authentication Identifier Generator's Private Key
740
Obtain Unique Platform Identifier
750
Transform Encrypted Platform Private Key To Generate Authentication Identifier Using Unique Platform Identifier
End

Fig. 7

Attorney's Docket No.: 042390.P6758

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

PROTECTED PLATFORM IDENTITY FOR DIGITAL SIGNING

the specification of which

☒ is attached hereto.
☐ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 USC 119
			☐ No ☐ Yes
			☐ No ☐ Yes
			☐ No ☐ Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:
William W. Schaal, Esq. Reg. No. 39,018, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
(Name of Attorney or Agent)
12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:
William W. Schaal, (714) 557-3800.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (Given name, family name): Paul C. Drews

Inventor's Signature: Paul C. Drews Date: 6-29-2000

Residence: Gaston, Oregon USA (City, State) Citizenship: USA (Country)

P. O. Address: 2390 NW Phillips Road

Gaston, Oregon 97119 USA

Full Name of Second/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

_____

Full Name of Third/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

_____

Full Name of Fourth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

_____

Full Name of Fifth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

_____

Full Name of Sixth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

P. O. Address _____

_____

Full Name of Seventh/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

P. O. Address _____

_____

Full Name of Eighth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

P. O. Address _____

_____

Full Name of Ninth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

P. O. Address _____

_____

Full Name of Tenth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

P. O. Address _____

_____

Full Name of Eleventh/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

P. O. Address _____

_____

APPENDIX A

I hereby appoint BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, a firm including: William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; Amy M. Armstrong, Reg. No. 42,265; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. 44,587; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George L. Fountain, Reg. No. 36,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. 41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Darren J. Milliken, Reg. No. 42,004; Chun M. Ng, Reg. No. 36878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Lisa A. Norris, Reg. No. 44,976; Daniel E. Ovanezian, Reg. No. 41,236; William P. Ryann, Reg. No. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey S. Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; James M. Wu, Reg. No. 45,241; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my attorneys; and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; and John F. Travis, Reg. No. 43,203; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (714) 557-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. 44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.